

Beyond The Bullet The ethics of war in cyberspace

By Jon Drahos

Contents

- ▶ What is cyberwarfare?
- ▶ Important terms
- ▶ Current use of cyberwarfare
- ▶ Ethical implications of cyberwarfare
- ▶ The future
- ▶ Conclusion

What is cyberwarfare?

- ▶ Not defined in a dictionary
 - ▶ Society often lags behind new technologies
 - ▶ Some argue that there is no "cyberwar"
- ▶ Attempt to piece together a definition

What is cyberwarfare? cont.

- ▶ Dictionary.com, cultural dictionary:
 - ▶ "The use of computers and other devices to attack an enemy's information systems as opposed to an enemy's armies or factories"
 - ▶ Who is attacking whom?
 - ▶ What motivations?
 - ▶ How?

What is cyberwarfare? cont.

- ▶ Wikipedia/ Richard A. Clarke:
 - ▶ "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption"
 - ▶ Between two parties, nation-states
 - ▶ Attack through computer networks?
 - ▶ Target : computer systems or others

What is cyberwarfare? cont.

- ▶ How is it different from other attacks?
 - ▶ Participants:
 - ▶ Not single hackers
 - ▶ Organized groups, often instructed by government
 - ▶ Motivation:
 - ▶ Not greed or curiosity of system
 - ▶ Political
 - ▶ Actions:
 - ▶ No physical activity needs to happen (no bombs, no airplanes, etc.)
 - ▶ Attacks need only happen through computers and computer networks

Important Terms

- ▶ **Botnet**
 - ▶ A group of computers that have been, usually unknowingly to the user, taken over by a hacker
 - ▶ "Recruited" by computer owner downloading a Trojan horse or other piece of malware
 - ▶ Can be controlled by the hacker to do whatever they want
 - ▶ Botnets time often sold on black market
 - ▶ Conficker worm: 5 million computers
 - ▶ Has potential to take down almost any nation's internet-connected infrastructure.

▶

Important Terms

- ▶ **DDoS (distributed denial of service)**
- ▶ **How it works:**
 - ▶ Infected computer (zombie) receives command from hacker over internet.
 - ▶ Zombie sends a request to connect (usually over TCP/IP) to server
 - ▶ Server receives request and reserves a bit of memory for zombie. Server waits for zombie to reply
 - ▶ Zombie sends another request to connect...
 - ▶ Thousands or more zombies make requests to server at the same time
 - ▶ Server crashes. Legitimate users blocked from server.....

▶

Important Terms

- ▶ **Zero-day vulnerability**
 - ▶ An exploit in a system (often an operating system) that no one has knowledge of
 - ▶ Element of surprise (massive damage)
 - ▶ Very valuable on the black market

▶

Current Situation

- ▶ **China**
 - ▶ Current structure and strategy never confirmed by the government
 - ▶ Suspected of having a de-centralized approach
 - ▶ Hackers join certain hacking groups
 - School groups, patriot hackers, online boards
 - ▶ Groups receive commands from Chinese military officers
 - ▶ Officers get orders from higher up

▶

Operation Aurora

- ▶ **Big cyberattack happened in mid 2009 to December 2009**
- ▶ **Attacked 20-30 companies**
- ▶ **Purpose?**
 - ▶ Modify source code in repositories
 - ▶ Steal trade secrets
 - ▶ Read email of Chinese human rights activists
- ▶ **Tracked down to two Chinese schools one with connections to military**
 - ▶ Shanghai Jiaotong University
 - ▶ the Lanxiang Vocational School
- ▶ **Unknown if orchestrated by government or simply student hackers**

▶

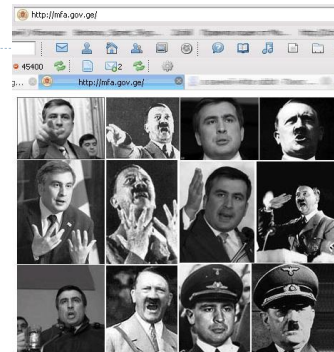
Current Situation

- ▶ **Russia**
 - ▶ Somewhat more structured than China
 - ▶ Structured under Federal Security Service, formerly part of KGB
 - ▶ Little information on capabilities
 - ▶ Booming black market for botnets and other malware

▶

Cyberwar on Estonia

- ▶ "First cyberwar" 2007, Estonian gov't moved a bronze Soviet statue from central square to outskirts
- ▶ Russians very upset
- ▶ Estonia government web sites attacked and defaced, Russian IP addresses?
- ▶ Banking system damaged



Current Situation

- ▶ **United States**
- ▶ **Very structured**
 - ▶ United States Cyber Command (USCYBERCOM)
 - ▶ A subgroup of U.S. Strategic Command
 - ▶ Consists of four subgroups:
 - ▶ Army, Navy, Air Force, Marines
 - ▶ Each with their own defense component
 - ▶ Little information on what they do

Stuxnet

- ▶ Infected computers in Iran, India, Indonesia, and Pakistan
- ▶ Targeted only a specific group of computers
 - ▶ Spread using an infected USB stick
 - ▶ Siemens Programmable Logic Controller
 - ▶ An interface between a program and a machine that performs physical work
 - ▶ Likely target: Iran's Bushehr nuclear power plant

Stuxnet cont.

- ▶ **Caused physical damage**
 - ▶ Fooled employees into thinking machines were fine
 - ▶ Spun refiners too fast
 - ▶ Likely set back Iran's nuclear capabilities a couple of years
- ▶ **Highly sophisticated**
 - ▶ Limited spread number, only spread for 21 days
 - ▶ Contained four zero-day exploits for Windows XP
 - ▶ Equipped with two stolen, but valid, security certificates
 - ▶ Hides itself on computer and updates via peer-to-peer networking
 - ▶ Almost certainly developed by a nation, probably U.S.

Ethical Implications

- ▶ **Kantian – First categorical imperative**
 - ▶ Rule: cyberwarfare should be performed only upon non-essential platforms, like websites, in order to prevent loss of innocent life
 - ▶ All nations agree to abide
 - ▶ Purpose of cyberwarfare attack is to confuse or disrupt military
 - ▶ Nation A attacks Nation B
 - ▶ Massive cyberattack occurs on B's websites
 - ▶ Civilians of nation A unable to access emergency information posted on internet
 - ▶ Results in possible loss of innocent life
 - ▶ Contradicts the purpose of rule: to save lives

Ethical Implications

- ▶ **Kantian – Second categorical imperative**
 - ▶ Difficult to assess in a specific manner.
 - ▶ Broad general statement:
 - ▶ creating a difficulty for soldiers and civilians alike to access information on the Internet would be using them to attain the purpose of causing confusion
 - ▶ Using people as a means to an end



Ethical Implications

- ▶ **Act Utilitarian – worst-case**
 - ▶ Nation A sets a Stuxnet-like worm on nation B
 - ▶ Nation B suffers a nuclear meltdown
 - ▶ Benefits:
 - ▶ No bombs dropped
 - ▶ Less money needed for a defense budget
 - ▶ Nation A won quickly
 - ▶ Consequences:
 - ▶ Thousands or more are endangered by meltdown
 - ▶ Fear of technology
 - ▶ A's populace horrified along with B's
 - ▶ Productive land around nuclear plant wasted
 - ▶ Increased healthcare spending



Ethical Implications

- ▶ **Rule Utilitarian**
 - ▶ Rule: Cyberattacks only permitted when there are not a disproportionate number of civilians harmed
 - ▶ Much like the Geneva convention
 - ▶ Nation A vs Nation B
 - ▶ Nation A releases a worm on nation B
 - ▶ Worm spreads to civilian computers, via common OS vulnerability, who have worse protection than government
 - ▶ More civilians computers infected than military computers. Disproportionate



Ethical Implications

- ▶ **Social Contract theory**
 - ▶ All nations allowed to use cyberwarfare
 - ▶ Nation A not very dependent on technology
 - ▶ Nation B highly dependent
 - ▶ Because nation A not very dependent, they would accept the rule
 - ▶ As rational humans, leaders of nation B would reject rule because they are much more vulnerable to cyberattacks, while their enemies are not



The Future

- ▶ **Cyberwarfare will become a more important issue**
 - ▶ Currently mostly limited to website defacing or stealing information
 - ▶ Potential future attacks much more damaging
- ▶ **Stuxnet: just the beginning**
 - ▶ Hospitals, traffic lights, water purifiers, energy grid, etc.
- ▶ **Cyberwars are cheap!**
 - ▶ In 2003, Joint Taskforce budgeted only \$26 million with 122 employees
 - ▶ DoD budgeted \$379.3 billion with 1.4 million personnel
- ▶ **Cyberattacks will undoubtedly continue**



Conclusion

- ▶ **Cyberwarfare is unethical**
 - ▶ Programmers make mistakes
 - ▶ Any potential attacker could make a mistake that could harm innocent people unintentionally
 - ▶ Disproportionate number of civilians could be hurt
- ▶ **Firm international laws need to be enacted**
 - ▶ Specifically outlawing some or all of cyberattacks
- ▶ **Every country needs to invest in cyber security.**
 - ▶ Every person should be aware of the potential consequences of cyberwarfare and how they can prevent it



Bibliography

- » Clarke, Richard A. "Cyber War". New York, NY: HarperCollins, 2010
 - » "Dictionary.com", 2011, 10 Mar, 2011. <<http://dictionary.com>>
 - » Greengard, Samuel. "The New Face of War." *Communications of the ACM*, Vol.53 no.12, pp20-22, December 2010. ACM Digital Library, 10 Mar, 2011 <<http://portal.acm.org>>
 - » Janczewski, Lech J., and Colarik, Andrew M. *Cyber Warfare and Cyber Terrorism*. Hershey, PA: IGI Global, 2008. <<http://books.google.com>>
 - » Laprise, J. "Cyber-warfare seen through a mariner's spyglass." *Technology and Society Magazine*, IEEE, vol.25, no.3, pp.26-33, Fall 2006. IEEE Xplore Digital Library, 15 Mar, 2011 <<http://ieeexplore.ieee.org>>
 - » Lesk, M. "The New Front Line: Estonia under Cyberassault." *Security & Privacy*, vol.5, no.4, pp.76-79, July-Aug. 2007. IEEE Xplore Digital Library, 20 Mar, 2011 <<http://ieeexplore.ieee.org>>
 - » Markoff, John "2 China Schools Said to Be Tied to Online Attacks" New York Times 18 Feb 2010
 - » Stapleton-Gray, Ross, and Woodcock, Bill. "National Internet Defense – Small States on the Skirmish Line." *Communications of the ACM*, Vol.54, no.3, pp.50-55, March 2011. ACM Digital Library, 15 Mar, 2011 <<http://portal.acm.org>>
 - » "U.S. Strategic Command". 2011, 25 Mar, 2011. <http://www.stratcom.mil/factsheets/Cyber_Command>
 - » Vasilev, D. "The Shadownet." *Engineering & Technology*, vol.5, no.16, pp.19-22, October 2010. IEEE Xplore Digital Library, 15 Mar, 2011 <<http://ieeexplore.ieee.org>>
-

